REMARKS

The Examiner has rejected the claims currently under consideration. Namely claims 28 through 35 have been rejected by the Examiner either under 35 U.S.C. 102 or 35 U.S.C. 103 in view of U.S. patent 5,265,164 to Matyas.

Rejections Under 35 U.S.C. §102

More particularly claims 28 and 30 have been rejected under 35 U.S.C. 102(b) as disclosing all the limitations of the claims on file in particular with reference to column 30, lines 15 to 38 of Matyas.

The present application and the claims under consideration are directed to a method of generating a set of session pairs for use of a private key and a public key in a public key cryptographic scheme. In the method, a set of session pairs, that is, the private key and corresponding public key, are established and then one of the pairs in this set is selected. This selected pair is processed by a predetermined function to generate a new session pair and the new session pair is then incorporated back into the set. In this way the session pairs in the set are constantly being updated.

The Matyas reference relates to a system which replicates a cryptographic facility. Replicating the cryptographic facility involves securely copying keys from one cryptographic facility to another so that if the first facility becomes inoperative, the second facility can be used instead. In the portion of the reference cited by the Examiner, namely column 30, lines 15 to 38, a cryptographic key KK1 is generated as a 128-bit key. The key generation algorithm uses a random number generator to produce the key. Two master keys KM and KMP are utilized with

the new key KK1 depending on predetermined parameters of the master key. A new cryptographic key KK2 is obtained from the first cryptographic key KK1 .

The system shown in the Matyas reference is a symmetric key system and does not discuss the provision of multiple key pairs. Claim 28 is specifically directed to the generation of session pairs for use as a private key and a public key in a public key cryptographic scheme and requires the establishment of a set having a plurality of session pairs, that is, a plurality of private keys and their corresponding public keys. Such a method is not described in the Matyas reference where there is no suggestion of session pairs or of sets of session pairs comprising private keys and corresponding public keys.

Claim 28 further requires a selection of one of the session pairs and processing that pair by a predetermined function to generate a new session pair. Again in Matyas there is no session pair for selection and this step is not found.

The final step required in claim 28 is the incorporation of the new session pair into the set which, by implication if not by explicit reference, requires the newly generated session pair to be available for selection in subsequent generation steps. Again, there is nothing disclosed in the reference of the addition of the newly generated key KK2 into a set from which further selections can be made.

Quite clearly therefore, claim 28 is not anticipated as required under 35 U.S.C. 102(b). Claim 30 depends from claim 28.

It is believed therefore that claims 28 and 30 clearly and patentably distinguish over the art as applied under 35 U.S.C. 102(b) and as such are in condition for allowance.

Rejections Under 35 U.S.C. §103

The Examiner has rejected the balance of the claims (claims 29 and 31-35) under 35 U.S.C. 103(a), all of which depend from and serve to further limit and define the invention set forth in claim 28.

As stated previously, the fundamental concept in Matyas is different from that disclosed and claimed in claim 28. Matyas generates a new key from its random number generator and may or may not modify that key depending upon the parameters of a pair of master keys. The resultant key is then used and deleted. Because the random number generated in Matyas could in fact be the resultant key, the random number generator must be of a high enough standard to maintain the integrity of such key generation.

By contrast, the present invention contemplates the provision of a set of keys on, for example, a smart card, which may then be combined to produce new keys while refreshing the set from which the keys are generated. A particular utility for this technique is in the area of smart cards which have low computing power and low cost and certainly do not contemplate the provision of random number generators of the caliber required to ensure security in the generation of session keys. As such, the teachings of Matyas provide no motivation for its adoption within the particular field to which the present invention relates and would not be useful in determining how to solve the problem of providing a large number of keys in a relatively small storage device.

With respect to claim 29, the Examiner suggests that Matyas teaches the selection of one of the session pairs a plurality of times. However, Matyas does not teach such an arrangement but rather teaches the generation of a new key from the random number generator at each key generation session. The incorporation of the newly generated session pair into the set for

subsequent selection is not taught by Matyas and therefore cannot render claim 29 obvious under 35 U.S.C 103.

The Examiner has also rejected claims 31 and 32 under 35 U.S.C. 103 on the basis that the use of a random number generator is well known. Matyas discloses a use of random number generator, but not to select which of a set of pairs would be used but in fact to generate a session key. There is no disclosure in Matyas or in any other reference made of record by the Examiner of selection of a set of pairs. In order for the Examiner to take official notice of a feature, it is believed that he must establish the basis for such official notice and he has not done so nor provided any indication of where it is well known to utilize a random number generator to select one of a set of key pairs. In the absence of such a teaching, it is believed there is no suggestion in the art made of record to utilize the random number generator in this manner and as such claims 31 and 32 clearly and patentably distinguish over the art.

Similarly with respect to claims 33 to 35, the Examiner does not indicate on what basis official notice is taken and as such, it is believed that in the absence of teaching it is inappropriate to reject the claims on file. Those claims distinguish over the art of record which suggests no motivation to utilize the steps recited in these claims and as such are believed to be in condition for allowance.

CONCLUSION

For the reasons pointed out above, Applicants believe that the application is in condition for allowance and such action is respectfully solicited. Should any issues remain unresolved, Examiner Peeso is invited to telephone the undersigned attorney.

Respectfully submitted,

RONALD C. MULLIN ET AL.

Lawrence A. Maxham
Agent for Applicant
Registration No. 24,483

THE MAXHAM FIRM
Symphony Towers
750 'B' Street, Suite 3100
San Diego, California 92101

Telephone: (619) 233-9004
Facsimile: (619) 544-1246